Firewall Log Analyzer and Monitoring Tool

Recommended Technology Stack and ML Algorithms

Recommended Architecture

Frontend: React.js, HTML, CSS
Backend: FastAPI (Python)
Database: MongoDB Atlas
Alerting: Email (SMTP)

Why FastAPI + React?
FastAPI is ideal for cybersecurity projects because it provides high performance, asynchronous request handling, and seamless integration with Machine Learning libraries. React offers a modern and interactive dashboard for real-time monitoring.

Why Not MERN with Multiple Backends?
Using both Node.js and FastAPI increases system complexity and is difficult to justify in a final-year project. Since Machine Learning and log analysis are best handled in Python, a single FastAPI backend is sufficient and efficient.

Recommended ML / AI Techniques

1. Rule-Based Detection:
Detects known attacks such as brute-force SSH attempts, port scanning, and unauthorized access using predefined rules.

2. Isolation Forest:
An unsupervised anomaly detection algorithm used to identify abnormal firewall log patterns without labeled data.

3. K-Means Clustering (Optional):
Groups similar traffic behavior to differentiate normal and suspicious activity patterns.

Viva Explanation:
The system follows a hybrid detection approach where rule-based methods detect known attacks and Isolation Forest identifies unknown anomalies, improving detection accuracy and reducing false positives.